Common Criteria

From Criteria to Requirements

A Strategy for Engaging Industry

Dr. Stuart Katzke

Sr. Research Scientist, NIST

skatzke@nist.gov

National Information Assurance Partnership:

National Institute of Standards and Technology

and

National Security Agency

Presentation Contents

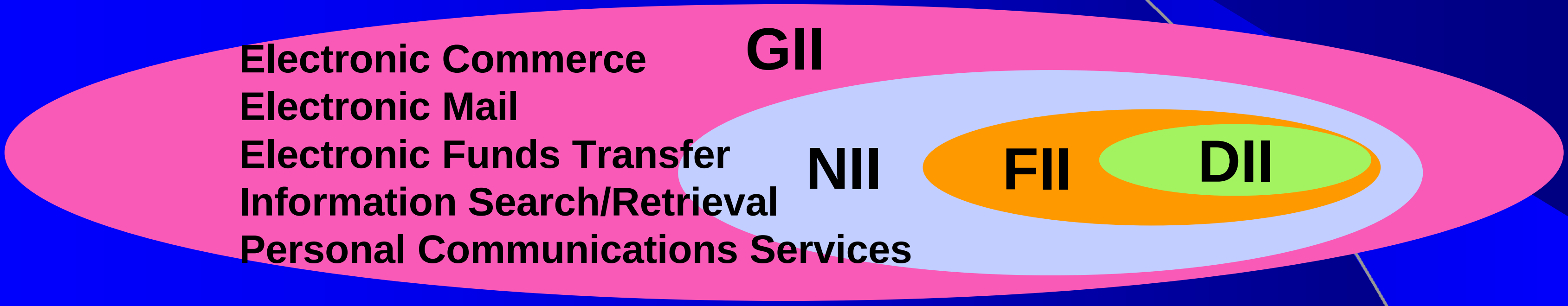
- Critical infrastructure protection
- Enterprise information assurance (IA)
- IA hard problem areas
- Role of evaluated technology
- Common criteria (CC) project
- CC recognition arrangement (CCRA)
- Extending CC to systems
- NIAP program areas
- NIAP security requirements working groups

INFORMATION ASSURANCE: GLOBAL

Interlocking Global Critical Infrastructures:

- Finance
- Telecom
- Energy
- Transportation
- Water Supply
- Federal Govt
- DoD / Intel
- International

Served by Interlocking Information Infrastructures:



Electronic Commerce
Electronic Mail
Electronic Funds Transfer
Information Search/Retrieval
Personal Communications Services

AUTHENTICATION, INTEGRITY, AVAILABILITY, CONFIDENTIALITY, NON-REPUDIATION

Requiring Active Cyber Defense:

PROTECT **DETECT & REPORT** **RESPOND**

Common Criteria

INFORMATION ASSURANCE (IA): ENTERPRISE

ACTIVE CYBER DEFENSE

PROTECT DETECT & REPORT RESPOND

Layered Defense-in-Depth

Attack Sensing & Warning

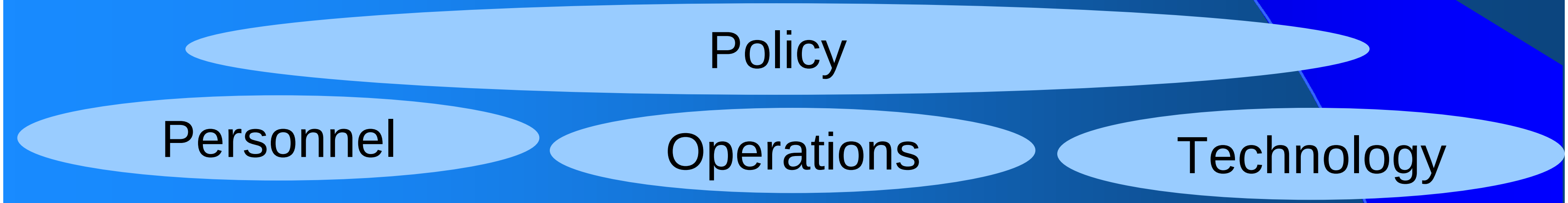
Data Fusion & Analysis

Attribute
- Source
- Sponsor
- Intent
- Impact

Restore

Pursuit
- Prosecute US Crime
- Retaliate Foreign Attack (high risk)

Via



Personnel
- Cyber Security Awareness
- Training & Certification
  - –security administrators
  - –security engineers
  - –security assessors

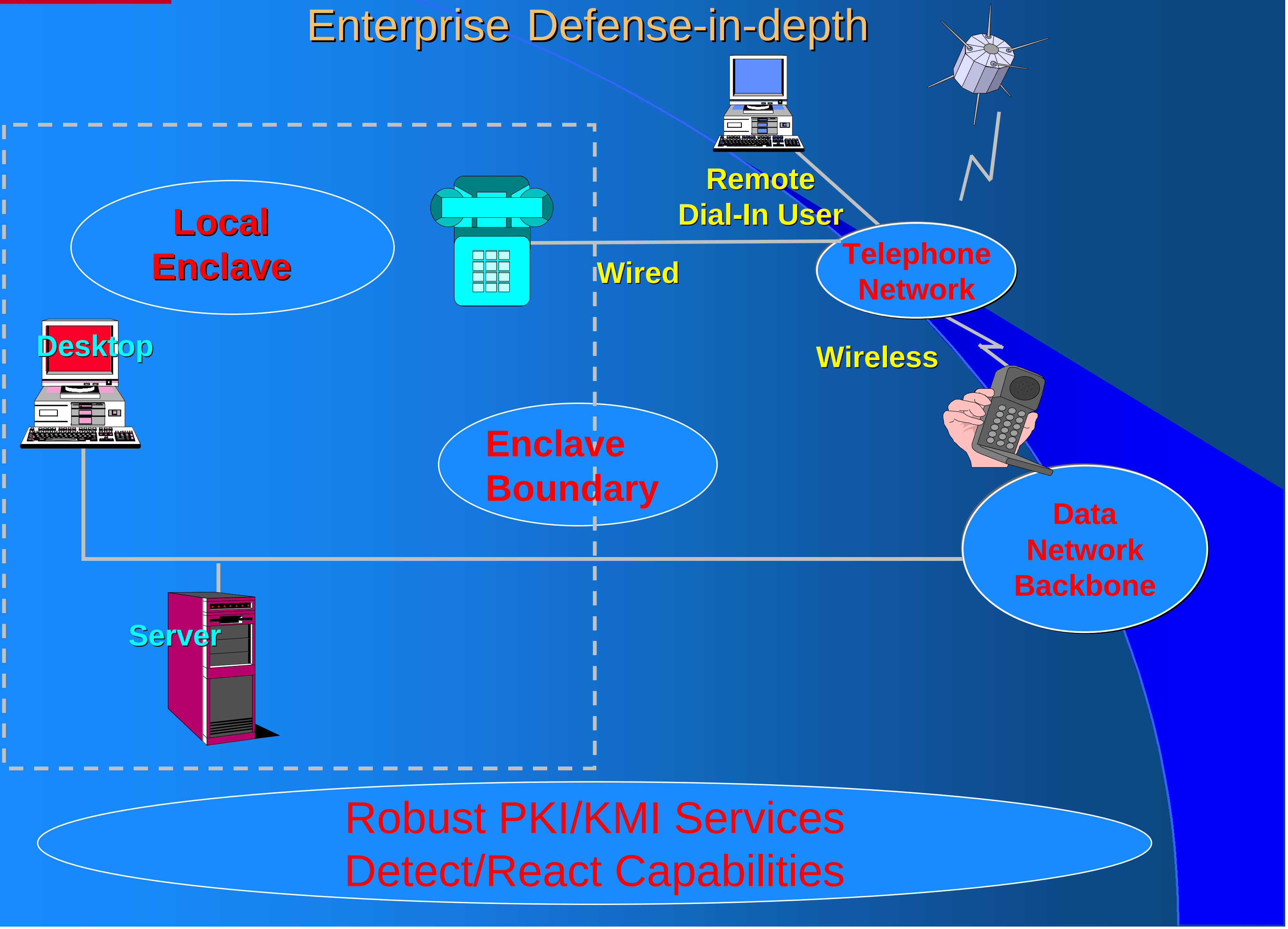
Operations
- Cyber Situational Awareness
  - - Attack Sensing & Warning
  - - Coordinated Response
- Cyber Operational Readiness Assessments
- Support to Exercises

Technology
- Strong Cryptography
  - - Digital Signature
  - - Encryption
- Security Enabled COTS & GOTS IT
- Key Mgt. Infrastructure
- Intrusion Detectors
- Assessment Tools

Common Criteria

IA Solutions Environment

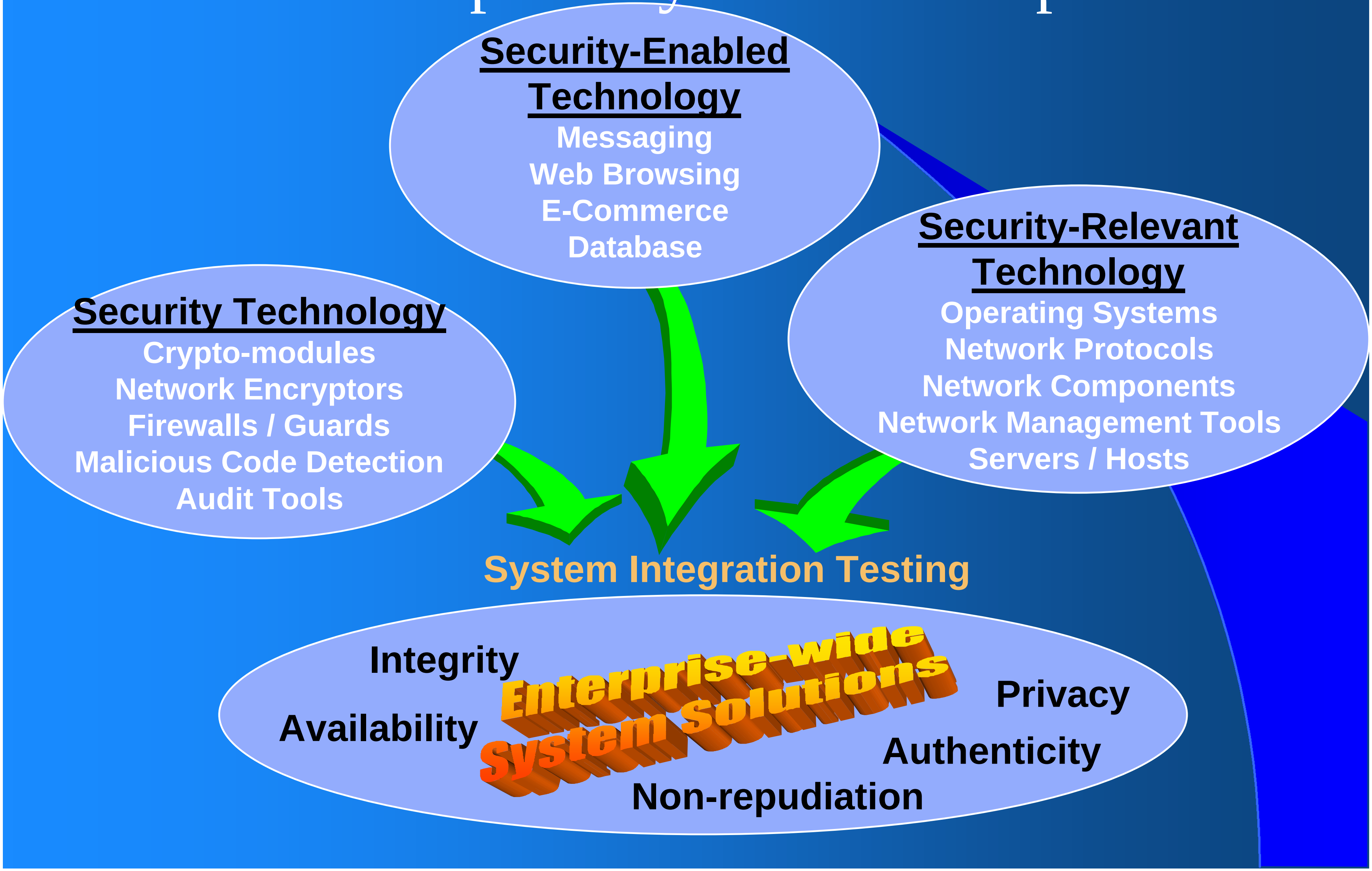
Enterprise Defense-in-depth



Robust PKI/KMI Services
Detect/React Capabilities

Common Criteria

Information Assurance in Enterprise System Development



Security-Enabled Technology

Messaging
Web Browsing
E-Commerce
Database

Security-Relevant Technology

Operating Systems
Network Protocols
Network Components
Network Management Tools
Servers / Hosts

Security Technology

Crypto-modules
Network Encryptors
Firewalls / Guards
Malicious Code Detection
Audit Tools

System Integration Testing

Enterprise-wide System Solutions

Integrity
Availability
Privacy
Authenticity
Non-repudiation

Enterprise IA: Today's Situation (1)

- Convincing organizations/people there is a problem
- Convincing them to do something about the problem
- Typical reasons why they don't do something
  - It won't/hasn't happen to me (or has not hurt me too bad)
  - I don't know how (too hard, complex, technical)
  - Security gets in the way of (performance, usability,…)
  - I'm not cyber-connected, I'm isolated
  - It's not my responsibility (security staff do that)
  - It costs too much
  - I'll accept the risk

Enterprise IA: Today's Situation (2)

- Passwords still primary method of authentication
  - OK when used securely
  - But, often not used securely
- Plethora of security solutions (good news/bad news)
- Very little "plug & play" security compatibility
- Vulnerability identification & patching still not being done (icat.nist.Gov/icat.cfm)
- Intrusion detection/attack sensing, warning, & response need improvement

Enterprise IA: Today's Situation (3)

- **Security management practices**
  - **No/poor comprehensive enterprise security policy**
  - **Poor personnel awareness, training, education**
  - **Security not *really* part of performance plans**
  - **Poor backup/disaster recovery planning**
  - **No/weak personnel background checks**
  - **Inadequate I&A practices (e.g., Passwords)**

Enterprise IA: Today's Situation (4)

- Best practices
  - What are they? (Definitional/conceptual)
  - Implies "only" way (vs. accepted, common, suggested, recommended)
  - Credibility? (Authoritative sources, effectiveness)
  - Which should I use? (Appropriate, complete)
  - Where do I stop? (Scope, granularity)
  - Criteria for assessing conformance?

Common Criteria

IA Hard Problem Areas (1)

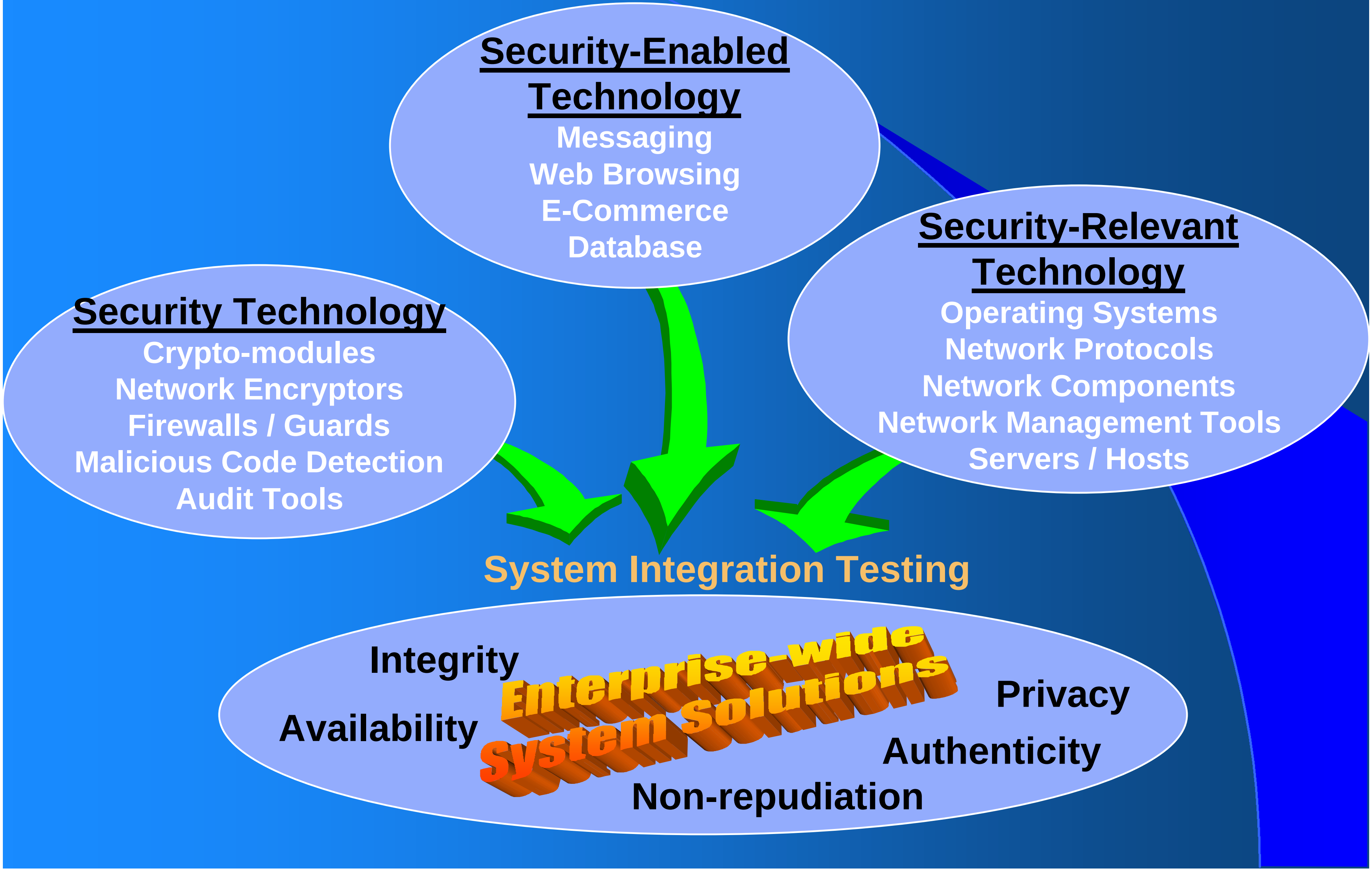
- National/international attack sensing, warning, & response
- Obtaining balance in CIP cooperation between governments & industry
- Rapidly changing technology & time to market pressures result in low assurance products (e.g., after market “patches”)
- Emerging technologies: functionality & performance more important than security

Common Criteria

IA Hard Problem Areas (2)

- Improving security metrics (products, systems, programs, competence)
- Improving ability to survive & recovery (from attacks/errors/events from both known/unknown sources)
- Improving techniques for security evaluation /certification & accreditation
- Improving techniques for secure system design & development/integration

Evaluated Technology



Security-Enabled Technology

Messaging
Web Browsing
E-Commerce
Database

Security Technology

Crypto-modules
Network Encryptors
Firewalls / Guards
Malicious Code Detection
Audit Tools

Security-Relevant Technology

Operating Systems
Network Protocols
Network Components
Network Management Tools
Servers / Hosts

System Integration Testing

Integrity
Availability
Enterprise-wide System Solutions
Privacy
Authenticity
Non-repudiation

What Is Needed?

- Producers of IT products need to have a better understanding of consumer’s information security requirements
- Consumers of IT products, systems, and networks need to have better ways to:
  - ✓ Specify desired security features and assurances
  - ✓ Assess the security claims made by producers

Common Criteria Project

The International Common Criteria Standard

ISO/IEC 15408

What the standard is –

- Common structure and language for expressing product/system IT security requirements (part 1)
- Catalog of standardized IT security requirement components and packages (parts 2 and 3)

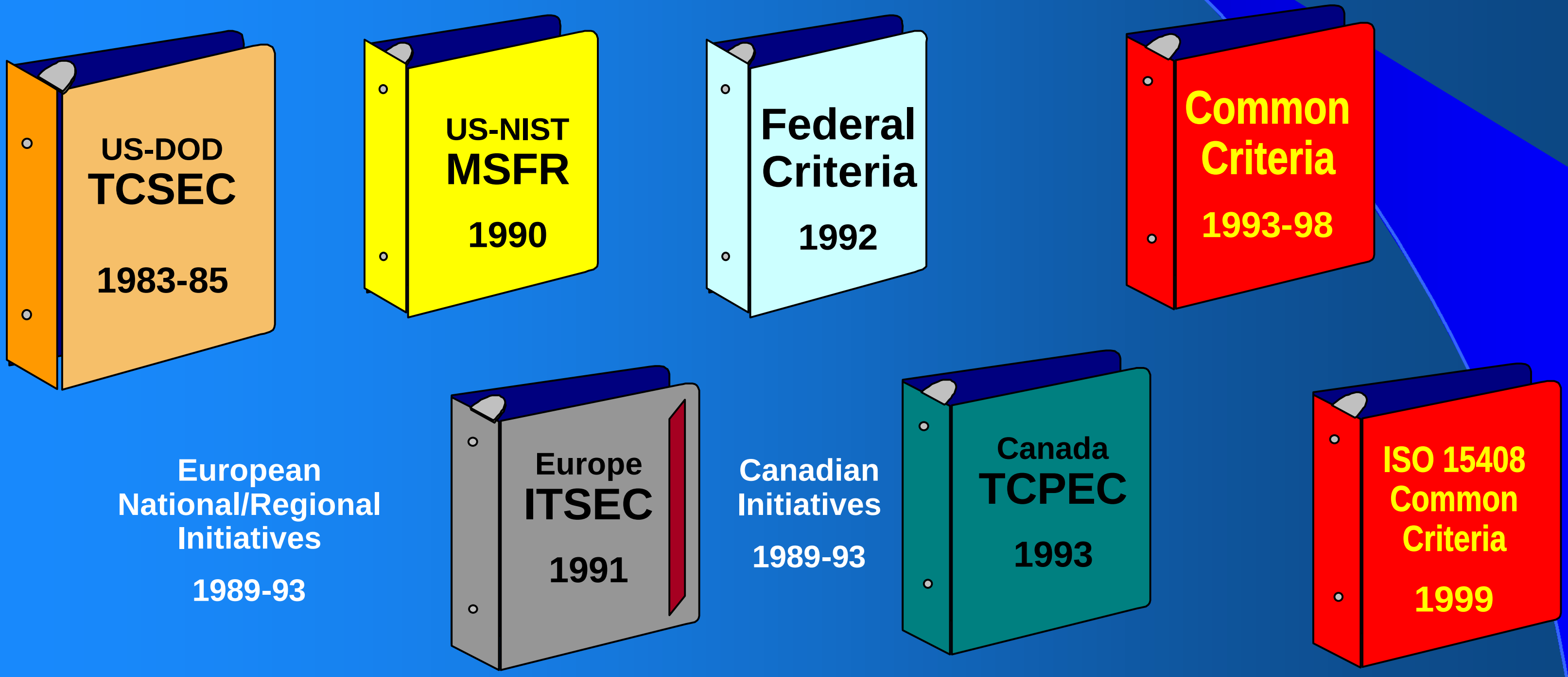
How the standard is used –

- Develop protection profiles and security targets -- specific IT security requirements and specifications for products and systems
- Evaluate products and systems against known and understood IT security requirements

Common Criteria

An Evolutionary Process

Two decades of research and development…



US-DOD
TCSEC
1983-85

US-NIST
MSFR
1990

Federal Criteria
1992

Common Criteria
1993-98

European National/Regional Initiatives
1989-93

Europe
ITSEC
1991

Canadian Initiatives
1989-93

Canada
TCPEC
1993

ISO 15408
Common Criteria
1999

Objectives

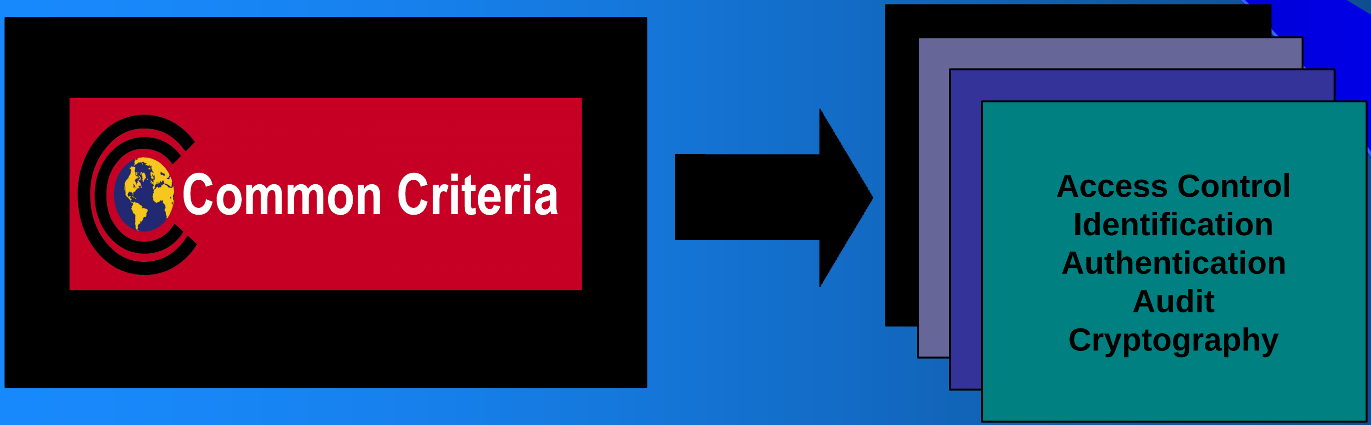
- Develop a single international IT product and system security specification criteria, or *common criteria (CC)*
- Adopt the CC as an international IT security standard under ISO
- Promote international recognition of IT product security evaluations
- Create a level international playing field for product and system developers
- Facilitate greater world-wide availability of security-capable IT products

Common Criteria

Defining Requirements

ISO/IEC Standard 15408

Protection Profiles



Access Control
Identification
Authentication
Audit
Cryptography

- ✓ Operating Systems
- ✓ Database Systems
- ✓ Firewalls
- ✓ Smart Cards
- ✓ Applications
- ✓ Biometrics
- ✓ Routers
- ✓ VPNs

A flexible, robust catalogue of standardized IT security requirements (features and assurances)

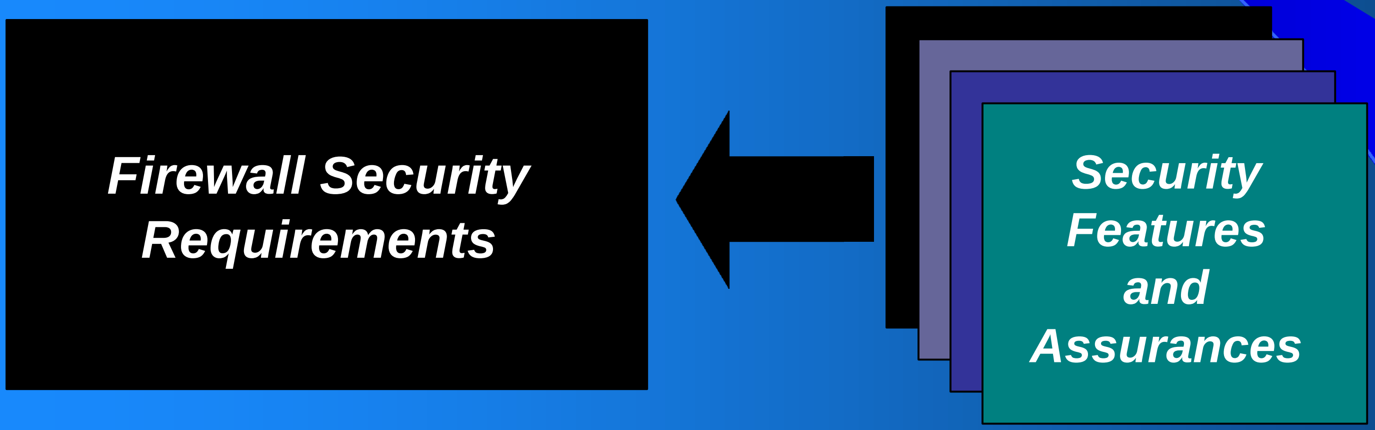
Consumer-driven security requirements in specific information technology areas

Common Criteria

Industry Responds

Protection Profile

Security Targets



Firewall Security Requirements

Security Features and Assurances

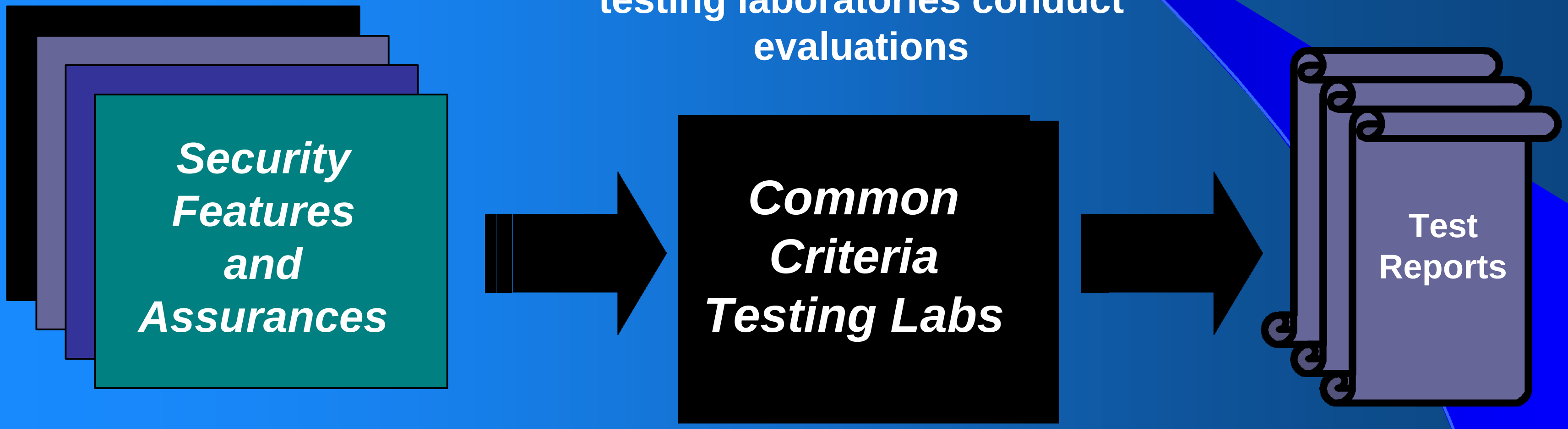
- ✓ CISCO Firewall
- ✓ Lucent Firewall
- ✓ Checkpoint Firewall
- ✓ Network Assoc. Firewall

Consumer statement of IT security requirements to industry in a specific information technology area

Vendor statements of security claims for their IT products

Demonstrating Conformance

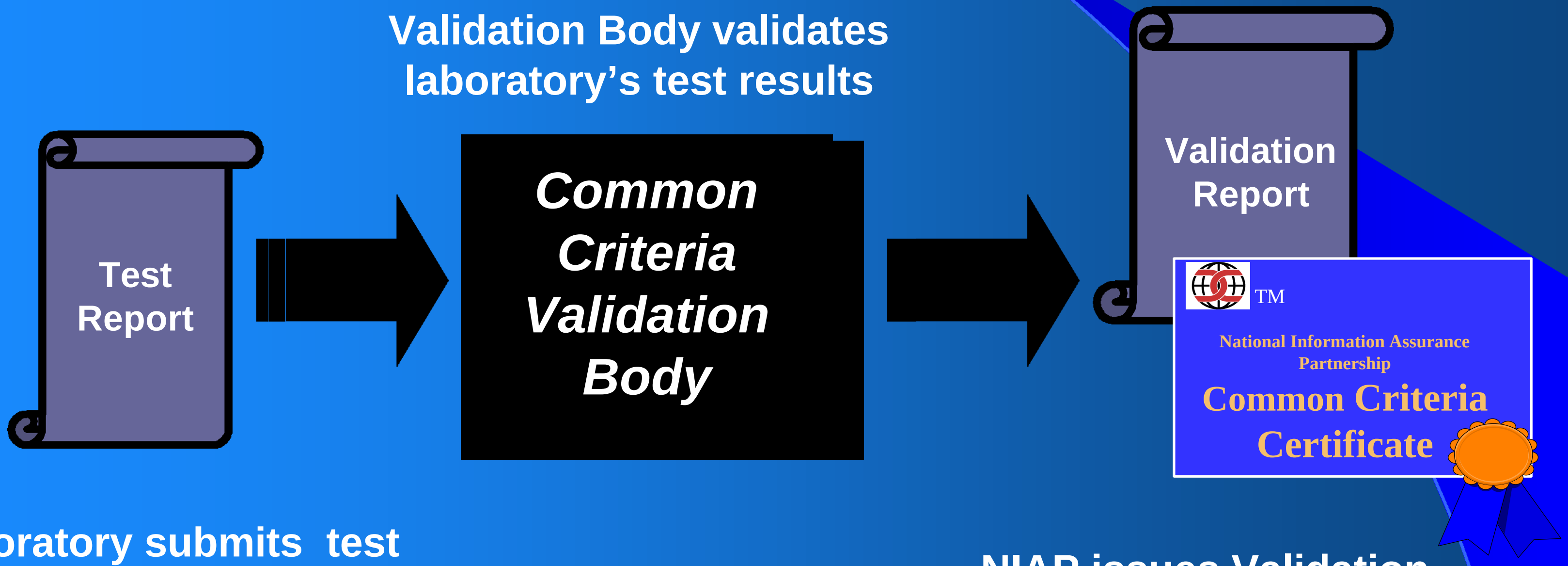
Private sector, accredited security testing laboratories conduct evaluations


Security Features and Assurances
Common Criteria Testing Labs
Test Reports

Vendors bring IT products to independent, impartial testing facilities for security evaluation

Test results submitted to NIAP for post-evaluation validation

Validating Test Results



Validation Body validates laboratory's test results

Test Report

Common Criteria Validation Body

Validation Report

TM

National Information Assurance Partnership

Common Criteria Certificate

Laboratory submits test report to Validation Body

NIAP issues Validation Report and Common Criteria Certificate

Common Criteria

CC Recognition Arrangement

CC Recognition Arrangement (CCRA) May 2000

Current members

Australia, Canada, Finland, France, Germany, Greece, Italy, the Netherlands, New Zealand, Norway, Spain, United Kingdom, United States

November 2000

Israel

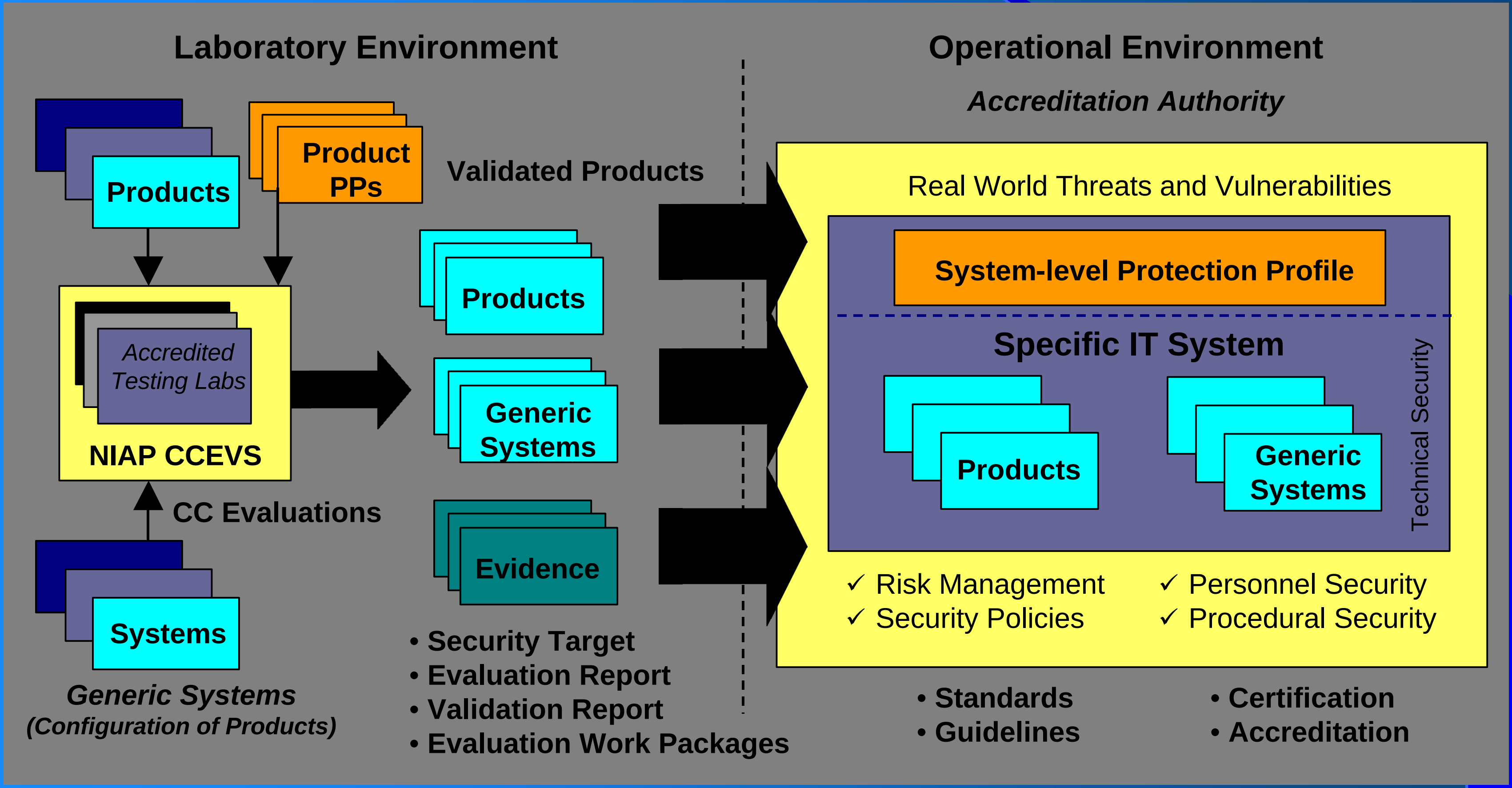
Potential future expansion

Japan, Korea, Russia, 2 Europe, 2 Asia-Pacific

Common Criteria

A Comprehensive Approach

Linking Critical Assessment Activities



- Security Target
- Evaluation Report
- Validation Report
- Evaluation Work Packages

✓ Risk Management
✓ Security Policies
✓ Personnel Security
✓ Procedural Security

- Standards
- Guidelines
- Certification
- Accreditation

Introducing NIAP

- The National Information Assurance Partnership (NIAP) is a U.S. Government initiative designed to meet the security testing, evaluation, and assessment needs of both information technology (IT) producers and consumers
- NIAP is a collaboration between the national institute of standards and technology (NIST) and the national security agency (NSA) in fulfilling their respective responsibilities under the computer security act of 1987

Program Areas

- **Security requirements definition and specification**

  How do we tell product and systems developers what types of IT security we want?

- **Product and system security testing, evaluation, and assessment**

  How do we know if developers produced what we asked for?

- **Information assurance research**

  How can we improve the ways we achieve assurance in our products and systems?

Common Criteria

Security Requirements Definition

- Promote the development of product-level Common Criteria protection profiles for key technology areas--e.g.,
  - Operating systems, database systems, firewalls
  - Telecommunications switches and smartcards
- Promote the development of systems-level Common Criteria protection profiles for key industry/constituency groups--e.g.,
  - Smart Card Users
  - Process Control
  - Healthcare industry

Common Criteria

NIAP Forums

(Technology Area and Industry Sector)

- Focus on security requirements definition
- Achieve results in community driven, cooperative environment
- Reach critical mass and rapid convergence on IT security requirements
  - **Raise security bar across the board; Increase later**
  - **May require compromise on less than optimal solutions**
  - **Contribute requirements to standards groups**

Forum Expectations

- Community ownership of security requirements
  - **Leadership**
  - **Funding/resources**
  - **Technical expertise**
- Community adoption and enforcement through acquisition
- Increased demand for evaluated IT products and systems

Common Criteria

Recent Forum Successes

- Smart card security users group
  (Technology area & industry sector)
- Healthcare security forum
  (Industry sector)
- Process control security requirements forum
  (Industry sector)
- Telecommunications security forum
  (Industry sector)

Potential Forums

- Technology areas
  - Operating systems
  - Database systems
  - Firewalls
  - Biometrics
- Industry sectors
  - Insurance
  - Audit and controls
  - Banking and finance
  - Manufacturing

Common Criteria

NIAP Invitation

- Looking for additional targets of opportunity
- Priority given to:
  - CIP-related areas/communities
  - Relevance to NIST & NSA constituents

IA Web URLs

- NIST information assurance activities www.itl.nist.gov/div893/
- NSA information assurance activities www.nsa.gov (see INFOSEC)
- National Security Telecommunications and Information Systems Security Committee (NSTISSC): www.nstissc.gov

IA Web URLs

- CC/NIAP: niap.nist.gov
- CC Tool Box (trade mark) & CC Profiling Knowledge Base (trade mark): niap.nist.gov/tools/cctool.html
- IATF: www.iatf.net
- Security Proof of Concept Keystone (SPOCK): www.coact.com/spock.html

Contact Information

National Information Assurance Partnership
100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

Director	***Deputy Director***	**Sr. *Technical Advisor***
Dr. Ron S. Ross	**Terry Losonsky**	**Dr. Stu Katzke**
NIST-ITL	**NSA-V1**	**NIST-ITL**
(301) 975-5390	**(301) 975-4060**	**(410) 854-4458**
rross@nist.gov	**tmloson@missi.ncsc.mil**	**skatzke@nist.gov**

Email: niap-info@nist.gov
World Wide Web: http://niap.nist.gov